139A-NY-C262228-95

SEARCHED INDEXED
SERIALIZED FILED
NOV 0 2 1998

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 8 of 28

****

The Wonderful World of Pagers

by Erik Bloodaxe

Screaming through the electromagnet swamp we live in are hundreds of thousands of messages of varying degrees of importance. Doctors, police, corporate executives, housewives and drug dealers all find themselves constantly trapped at the mercy of a teeny little box: the pager.

Everyone has seen a pager; almost everyone has one. Over 20 million pagers are on the streets in the US alone, sorting out their particular chunk of the radio-spectrum. Another fifty-thousand more are put into service each day.

But what the hell are these things really doing? What more can we do with them than be reminded to call mom, or to "pick up dry-cleaning?"

Lots.

** PROTOCOLS **

Pagers today use a variety of signalling formats such as POCSAG, FLEX and GOLAY. The most common by far is POCSAG (Post Office Standardization Advisory Group), a standard set by the British Post Office and adopted world-wide for paging.

POCSAG is transmitted at three transmission rates--512, 1200 and 2400 bps. Most commercial paging companies today use at least 1200, although many companies who own their own paging terminals for in-house use transmit at 512. Nationwide carriers (SkyTel, PageNet, MobileComm, etc.) send the majority of their traffic at 2400 to make the maximum use of their bandwidth. In other words, the faster they can deliver pages, the smaller their queue of outgoing pages is. Although these carriers have upgraded their equipment in the field to broadcast at 2400 (or plan to do so in the near future), they still send out some pages at 1200 and 512 to accommodate their customers with older pagers. Most 512 and 1200 traffic on the nationwide services is numeric or tone-only pages.

POCSAG messages are broadcast in batches. Each batch is comprised of 8 frames, and each frame contains two codewords separated by a "synchronization" codeword. A message can have as many codewords as needed to deliver the page and can stretch through several batches if needed. The end of a complete message is indicated by a "next address" codeword. Both addressing and user data are sent in the codewords, the distinction being the least significant bit of the codeword: 0 for address data, and 1 for user-data.

Standard alphanumeric data is sent in a seven-bit format, with each codeword containing 2 6/7 characters. A newer 8-bit alphanumeric format is implemented by some carriers which allow users to send data such as computer files, graphics in addition to regular alphanumeric messages. The 8 bit format allows for 2.5 characters per codeword.

Numeric data is 4 bit, allowing up to 5 numbers to be transmitted per codeword. Tone and voice pages contain address information only.

(NOTE: Pager data uses BCH 32,21 for encoding. I don't imagine very many of you will be trying to decode pager data by building your own decoders, but for those of you who may, take my interpretation of POCSAG framing with a grain of salt, and try to dig up the actual POCSAG specs.)

** THE PAGING RECEIVER **

Paging receivers come in hundreds of shapes and sizes, although the vast majority are manufactured by Motorola. Numeric pagers comprise over fifty percent all pagers in use. Alphanumeric comprises about thirty percent, with tone and voice pagers making up the remainder.

Pagers are uniquely addressed by a capcode. The capcode is usually six to eight digits in length, and will be printed somewhere on the pager itself. Many pager companies assign customers PIN numbers, which are then cross-referenced to a given capcode in databases maintained by the service provider. PIN numbers have no other relationship to the capcode.

Tone pagers are by far the most limited paging devices in use. When a specified number has been called, an address only message is broadcast, which causes the intended receiver to beep. Wow. Tone pagers usually have 4 capcodes, which can correspond to different locations to call back. Voice pagers are similar, except they allow the calling party to leave a 15 to 30 second message. The voice message is broadcast immediately after the capcode of the receiver, which unsquelches the device's audio.

Numeric pagers, although seemingly limited by their lack of display options have proven otherwise by enterprising users. Most numeric data sent is obviously related to phone numbers, but numerous users have developed codes relating to various actions to be carried out by the party being paged. The most prolific users of this have been the Chinese who have one of the most active paging networks in the world. I suppose the next biggest users of code-style numeric paging would be drug dealers. (2112 0830 187 -- get to the fucking drop site by 8:30 or I'll bust a cap in your ass!) :)

Alphanumeric pagers are most often contacted through a dedicated service that will manually enter in the message to be sent onto the paging terminal. One such service, NDC, offers its phone-answering and message typing services to various pager companies. Next time you are talking to a pager operator, ask him or her if they are at NDC. They probably are.

In addition to the capcode, pagers will have an FCC ID number, a serial number, and most importantly, the frequency that the device has been crystaled for imprinted on the back of the device. Although technology exists that would allow pagers to listen on a number of frequencies by synthesizing the frequency rather than using a crystal, pager manufacturers stick to using crystals to "keep the unit cost down."

Pagers may have multiple capcodes by which they can be addressed by. Multiple capcodes are most often used when a person has subscribed to various services offered by their provider, or when the subscriber is part of a group of individuals who will all need to receive the same page simultaneously (police, EMTs, etc.).

Most low-cost pagers have their capcode stored on the circuit board in a PAL. Most paging companies will completely exchange pagers rather than remove and reprogram the PAL, so I don't think it's worth it for any experimenter to attempt. However, like most Motorola devices, many of their paging products can be reprogrammed

with a special serial cable and software. Reprogramming software is usually limited to changing baud rates, and adding capcodes.

Additionally, some units can be reprogrammed over the air by the service provider. Using a POCSAG feature known as OTP (over the air programming) the service provider can instruct the paging receiver to add capcodes, remove capcodes, or even shut itself down in the case of non-payment.

** SERVICES **

With the growing popularity of alphanumeric pagers, many service providers have decided to branch out into the information business. The most common of these services is delivery of news headlines. Other services include stock quotes, airline flight information, voice mail and fax reception notification, and email. Of course, all of these services are available for a small additional monthly premium.

Email is probably the single coolest thing to have sent to your alpha pager. (Unless you subscribe to about a zillion mailing lists) Companies like SkyTel and Radiomail give the user an email address that automatically forwards to your paging device.
IE: PIN-NUMBER@skymail.com. Several packages exist for forwarding email from a UNIX system by sending stripping down the email to pertinent info such as FROM and SUBJECT lines, and executing a script to send the incoming mail out via a pager terminal data port.
One such program is IXOBEEPER, which can be found with an archie query.

Radiomail's founder, (and rather famous ex-hacker in his own right - go look at ancient ComputerWorld headlines), Geoff Goodfellow had devised such a method back in the late 70's. His program watched for incoming email, parsed the mail headers, and redirected the FROM and SUBJECT lines to his alphanumeric pager. Obviously, not many people had alphanumeric pagers at all, much less email addresses on ARPANET back in the 70's, so Geoff's email pager idea didn't see much wide-spread use until much later.

Two RFC's have been issued recently regarding paging and the Internet. RFC 1568, the Simple Network Paging Protocol, acts similarly to SMTP. Upon connecting to the SNPP port the user issues commands such as:

```
      PAGE followed by pager telephone number
      MESS followed by the alpha or numeric message
      SEND
    & QUIT
```

RFC 1568 has met with some opposition in the IETF, who don't consider it worthwhile to implement a new protocol to handle paging, since it can be handled easily using other methods.

The other RFC, number 1569, suggests that paging be addressed in a rather unique manner. Using the domain TPC.INT, which would be reserved for services that necessitate the direct connection to The Phone Company, individual pagers would be addressed by their individual phone numbers. Usernames would be limited to pager-alpha or pager-numeric to represent the type of pager being addressed. For example, an alpha-page being sent to 1-800-555-1212 would be sent as pager-alpha@2.1.2.1.5.5.5.0.0.8.1.tcp.int.

** PAGING TERMINAL DATA PORTS **

Many services offer modem connections to pager terminals so that computer users can send pages from their desks using software packages like WinBeep, Notify! or Messenger. All of these services connect to the pager terminal and speak to it using a protocol known as

along with every other device on the planet, right? Plug and Pray!)

The network will be layed out almost identically to MTEL's existing paging network, using dedicated lines to connect towers in an area to a central satellite up/downlink. One key difference will be the addition of highly somewhat sensitive receivers on the network, to pick up the ACKs and replies of the customer units, which will probably broadcast at about 2 or 3 watts. The most exciting difference will be the speed at which the network transmits data: 24,000 Kbps. Twenty-four thousand. (I couldn't believe it either. Not only can you get your GIFs sent to your pager, but you get them blinding FAST!) The actual units themselves will most likely look like existing alphanumeric pagers with possibly a few more buttons, and of course, PCMCIA units will be available to integrate with computer applications.

Beyond these advancements, other types of services plan on offering paging like features. CDPD, TDMA & CDMA Digital Cellular and ESMR all plan on providing a "pager-like" option for their customers. The mere fact that you can walk into a K-Mart and buy a pager off a rack would indicate to me that pagers are far to ingrained into our society, and represent a wireless technology that doesn't scare or confuse the yokels. Such a technology doesn't ever really go away.

** BIBLIOGRAPHY **

Kneitel, Tom, "The Secret Life of Beepers," _Popular Communications_, p. 8, July, 1994.

O'Brien, Michael, "Beep! Beep! Beep!," _Sun Expert_, p. 17, March, 1994.

O'Malley, Chris, "Pagers Grow Up," _Mobile Office_, p. 48, August, 1994.

** PAGER FREQUENCIES - US **

[Frequencies transmitting pager information are extremely easy to identify while scanning. They identify each batch transmission with a two-tone signal, followed by bursts of data. People with scanners may tune into some of the following frequencies to familiarize themselves with this distinct audio.]

Voice Pager Ranges:	152.01	- 152.21
	453.025	- 453.125
	454.025	- 454.65
	462.75	- 462.925
Other Paging Ranges:	35.02	- 35.68
	43.20	- 43.68
	152.51	- 152.84
	157.77	- 158.07
	158.49	- 158.64
	459.025	- 459.625
	929.0125	- 931.9875

** PAGER FREQUENCIES - WORLD **

Austria	162.050	- 162.075	T,N,A
Australia	148.100	- 166.540	T,N,A
	411.500	- 511.500	T,N,A
Canada	929.025	- 931-975	T,N,A
	138.025	- 173.975	T,N,A
	406.025	- 511.975	T,N,A
China	152.000	- 172.575	N,A
Denmark		469.750	N,A
Finland		450.225	T,N,A
	146.275	- 146.325	T,N,A
France	466.025	- 466.075	T,N,A
Germany	465.970	- 466.075	T,N,A
		173.200	T,N,A
Hong Kong		172.525	N,A
		280.0875	T,N,A
Indonesia	151.175	- 153.050	A
Ireland	153.000	- 153.825	T,N,A
Italy		466.075	T,N,A
		161.175	T,N
Japan	278.1625	- 283.8875	T,N
Korea	146.320	- 173.320	T,N,A
Malaysia	152.175	- 172.525	N,A,V
		931.9375	N,A
Netherlands	156.9865	- 164.350	T,N,A
New Zealand	157.925	- 158.050	T,N,A
Norway	148.050	- 169.850	T,N,A
Singapore		161.450	N,A
		931.9375	N,A
Sweden		169.8	T,N,A
Switzerland		149.5	T,N,A
Taiwan		166.775	N,A
		280.9375	N,A
Thailand		450.525	N,A
	172.525	- 173.475	N,A
UK	138.150	- 153.275	T,N,A
	454.675	- 466.075	T,N,A

T = Tone
N = Numeric
A = Alphanumeric

V = Voice

** INTERCEPTION AND THE LAW **

For many years the interception of pages was not considered an invasion of privacy because of the limited information provided by the tone-only pagers in use at the time. In fact, when Congress passed the Electronic Communications Privacy Act in 1986 tone-only pagers were exempt from its provisions.

According to the ECPA, monitoring of all other types of paging signals, including voice, is illegal. But, due to this same law, paging transmissions are considered to have a reasonable expectation to privacy, and Law Enforcement officials must obtain a proper court order to intercept them, or have the consent of the subscriber.

To intercept pages, many LE-types will obtain beepers programmed with the same capcode as their suspect. To do this, they must contact the paging company and obtain the capcode associated with the person or phone number they are interested in. However, even enlisting the assistance of the paging companies often requires following proper legal procedures (warrants, subpoenas, etc.).

More sophisticated pager-interception devices are sold by a variety of companies. SWS Security sells a device called the "Beeper Buster" for about $4000.00. This particular device is scheduled as a Title III device, so any possession of it by someone outside a law enforcement agency is a federal crime. Greyson Electronics sells a package called PageTracker that uses an ICOM R7100 in conjunction with a personal computer to track and decode pager messages. (Greyson also sells a similar package to decode AMPS cellular messages from forward and reverse channels called "CellScope.")

For the average hacker-type, the most realistic and affordable option is the Universal M-400 decoder. This box is about 400 bucks and will decode POCSAG at 512 and 1200, as well as GOLAY (although I've never seen a paging service using GOLAY.) It also decodes CTCSS, DCS, DTMF, Baudot, ASCII, SITOR A & B, FEC-A, SWED-ARQ, ACARS, and FAX. It takes audio input from any scanners external speaker jack, and is probably the best decoder available to the Hacker/HAM for the price.

Output from the M400 shows the capcode followed by T, N or A (tone, numeric or alpha) ending with the message sent. Universal suggests hooking the input to the decoder directly to the scanner before any de-emphasis circuitry, to obtain the true signal. (Many scanners alter the audio before output for several reasons that aren't really relevant to this article...they just do. :))

Obviously, even by viewing the pager data as it streams by is of little use to anyone without knowing to whom the pager belongs to. Law Enforcement can get a subpoena and obtain the information easily, but anyone else is stuck trying to social engineer the paging company. One other alternative works quite well when you already know the individuals pager number, and need to obtain the capcode (for whatever reason).

Pager companies will buy large blocks in an exchange for their customers. It is extremely easy to discover the paging company from the phone number that corresponds to the target pager either through the RBOC or by paging someone and asking them who their provider is when they return your call. Once the company is known, the frequencies allocated to that company are registered with the FCC and are public information. Many CD-ROMs are available with the entire FCC Master Frequency Database. (Percon sells one for 99 bucks that covers the whole country -

716-386-6015) Libraries and the FCC itself will also have this information available.

With the frequency set and a decoder running, send a page that will be incredibly easy to discern from the tidal wave of pages spewing forth on the frequency. (6666666666, THIS IS YOUR TEST PAGE, etc...) It will eventually scroll by, and presto! How many important people love to give you their pager number?

** THE FUTURE **

With the advent of new technologies pagers will become even more present in both our businesses and private lives. Notebook computers and PDAs with PCMCIA slots can make use of the new PCMCIA pager cards. Some of these cards have actual screens that allow for use without the computer, but most require a program to pull message data out. These cards also have somewhat large storage capacity, so the length of messages have the option of being fairly large, should the service provider allow them to be.

With the advent of 8-bit alphanumeric services, users with PCMCIA pagers can expect to receive usable computer data such as spreadsheet entries, word processing documents, and of course, GIFs. (Hey, porno entrepreneurs: beeper-porn! Every day, you get a new gif sent to your pagecard! Woo Woo. Sad thing is, it would probably sell.)

A branch of Motorola known as EMBARC (Electronic Mail Broadcast to A Roaming Computer) was one of the first to allow for such broadcasts. EMBARC makes use of a proprietary Motorola protocol, rather than POCSAG, so subscribers must make use of either a Motorola NewsStream pager (with nifty serial cable) or a newer PCMCIA pager. Messages are sent to (and received by) the user through the use of special client software.

The software dials into the EMBARC message switch accessed through AT&T's ACCUNET packet-switched network. The device itself is used for authentication (most likely its capcode or serial number) and some oddball protocol is spoken to communicate with the switch.

Once connected, users have the option of sending a page out, or retrieving pages either too large for the memory of the pager, or from a list of all messages sent in the last 24 hours, in case the subscriber had his pager turned off.

Additionally, the devices can be addressed directly via x.400 addresses. (X.400: The CCITT standard that covers email address far too long to be worth sending anyone mail to.) So essentially, any EMBARC customer can be contacted from the Internet.

MTEL, the parent company of the huge paging service SkyTel, is implementing what may be the next generation of paging technologies. This service, NWN, being administrated by MTEL subsidiary Destineer, is most often called 2-way paging, but is more accurately Narrowband-PCS.

The network allows for the "pager" to be a transceiver. When a page arrives, the device receiving the page will automatically send back an acknowledgment of its completed reception. Devices may also send back some kind of "canned response" the user programs. An example might be: "Thanks, I got it!" or "Why on Earth are you eating up my allocated pages for the month with this crap?"

MTEL's service was awarded a Pioneers Preference by the FCC, which gave them access to the narrowband PCS spectrum before the auctions. This is a big deal, and did not go unnoticed by Microsoft. They dumped cash into the network, and said the devices will be supported by Chicago. (Yeah,

IXO.

Upon connection, a pager terminal identifies itself with the following:

ID=

(I bet you always wondered what the hell those systems were)
Paging terminals default to 300 E71, although many larger companies now have dialups supporting up to 2400.

Many such systems allow you to manually enter in the appropriate information by typing a capital "M" and a return at the ID= prompt. The system will then prompt you for the PIN of the party you wish to page, followed by a prompt for the message you wish to send, followed by a final prompt asking if you wish to send more pages. Not every pager terminal will support a manual entry, but most do.

All terminals support the IXO protocol. As there are far too many site specific examples within the breadth of IXO, we will concentrate on the most common type of pager services for our examples.

[Sample IXO transaction of a program sending the message ABC to PIN 123
gleened from the IXOBeeper Docs]

Pager Terminal	YOU
	<CR>
ID=	
	<ESC>PG1<CR>
Processing - Please Wait	
	<CR>
<CR>	
ACK <CR>	
<ESC>[p <CR>	
	<STX>123<CR>
	ABC<CR>
	<ETX>17;<CR>
<CR>	
ACK <CR>	
	<EOT><CR>
<ESC>EOT <CR>	

The checksum data came from:

STX	000 0010
1	011 0001
2	011 0010
3	001 0011
<CR>	000 1101
A	100 0001
B	100 0010
C	100 0011
<CR>	000 1101
ETX	000 0011
	1 0111 1011

1 7 ; Get it? Get an ASCII chart and it will all make sense.

Note: Everything in the paging blocks, from STX to ETX inclusive are used to generate the checksum. Also, this is binary data, guys...you can't just type at the ID= prompt and expect to have it recognized as IXO. It wants specific BITS. Got it? Just checking...

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 4
Page 1 ~ b6; b7C; b7D; b7E;
Page 2 ~ b6; b7C; b7D; b7E;
Page 3 ~ b6; b7C; b7D; b7E;
Page 4 ~ b6; b7C; b7D; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/14/2003

Individual, who has agreed to testify, provided the following information:

[redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D
b7E

Investigation on 10/07&8/2003 at Santa Maria, CA (telephonica[illegible])

File # [redacted] Date dictated

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/11/2002

SOURCE, who is not in a position to testify, was in contact with SA [redacted] from 08/14/2002 to 09/11/2002 via email and telephone. SOURCE provided the following information: b6 b7C

[redacted] b6 b7C b7D

Investigation on 09/11/2002 at Chicago, Illinois

File # [redacted] Date dictated 09/11/2002 b6 b7C b7D b7E

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 6
Page 2 ~ b6; b7C; b7D; b7E;
Page 3 ~ b6; b7C; b7D; b7E;
Page 4 ~ Duplicate;
Page 5 ~ Duplicate;
Page 6 ~ Duplicate;
Page 7 ~ b6; b7C; b7D; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/12/2002

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via email and in person from 08/17/2002 to 09/12/2002 [redacted] SOURCE provided [redacted]

b6
b7C
b7D

Investigation on 09/12/2002 at Chicago, Illinois

File # [redacted] Date dictated 09/12/2002

by SA [redacted]

b6
b7C
b7D
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 3
Page 2 ~ Duplicate;
Page 3 ~ b6; b7C; b7D; b7E;
Page 4 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/12/2002

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via electronic mail on 08/23/2002. SOURCE provided the following information: b6 b7C b7D

[redacted]

Investigation on 09/12/2002 at Chicago, Illinois

File # [redacted] Date dictated 09/12/2002 b6 b7C b7D

by SA [redacted] b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 1
Page 2 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/20/2002

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via electronic mail (email) and telephone regarding [redacted] SOURCE provided the following information: b6 b7C b7D

[redacted]

[redacted] b6 b7C b7D

[redacted]

[redacted]

Investigation on 08/20/2002 at Chicago, Illinois

File # [redacted] Date dictated 08/20/2002 b6 b7C b7D b7E

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 1
Page 2 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/19/2002

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via electronic mail (email) regarding [redacted] SOURCE provided the following information: b6 b7C b7D

[redacted]

Investigation on 08/19/2002 at Chicago, Illinois

File # [redacted] Date dictated 08/19/2002 b6 b7C b7D b7E

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 2
Page 2 ~ Duplicate;
Page 3 ~ b7D; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/05/2002

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via electronic mail (email) on 07/21/2002 regarding [redacted] SOURCE provided the following information: b6 b7C b7D

[redacted]

[redacted] b6 b7C b7D

[redacted]

[redacted]

Investigation on 08/05/2002 at Chicago, Illinois

File # [redacted] Date dictated 08/05/2002 b6 b7C b7D b7E

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 1
Page 2 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

2,3,5-7

Date of transcription 08/02/2002

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via electronic mail (email), telephone, and personal conversation from 08/01/2002 to 08/02/2002 regarding [redacted] SOURCE provided the following information: b6 b7C b7D

[redacted]

[redacted] b7D

[redacted]

[redacted]

Investigation on 08/02/2202 at Chicago, Illinois

File # [redacted] Date dictated 08/02/2002

by SA [redacted]

b6 b7C b7D b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted] [redacted] (REIEF)

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 5
Page 3 ~ b6; b7C; b7D; b7E;
Page 4 ~ b7D; b7E;
Page 6 ~ b6; b7C; b7D; b7E;
Page 7 ~ b6; b7C; b7D; b7E;
Page 9 ~ b6; b7C; b7D; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/30/2002

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via electronic mail (email) and telephone from 07/11/2002 to 07/29/2002 regarding [redacted] b6 b7C b7D

SOURCE provided the following information:

[redacted]

[redacted]

[redacted] b6 b7C b7D

[redacted]

[redacted]

[redacted]

[redacted]

Investigation on 07/29/2002 at Chicago, Illinois

File # [redacted] Date dictated 07/30/2002 b6 b7C b7D

by SA [redacted] b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 5
Page 4 ~ b6; b7C; b7D; b7E;
Page 5 ~ b6; b7C; b7D; b7E;
Page 6 ~ b6; b7C; b7D; b7E;
Page 7 ~ b6; b7C; b7D; b7E;
Page 8 ~ b6; b7C; b7D; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/18/2002

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via electronic mail (e-mail) and telephone on 07/17/2002 regarding [redacted] SOURCE provided the following information: b6 b7C b7D

[redacted]

[redacted] b6 b7C b7D

[redacted]

Investigation on 07/17/200[redacted] at Chicago, Illinois

File # [redacted] Date dictated 07/18/2002 b6 b7C b7D b7E

by SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 2
Page 2 ~ Duplicate;
Page 3 ~ b6; b7C; b7D; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/19/2002

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via electronic mail (e-mail) and telephone regarding [redacted] SOURCE provided the following information: b6 b7C b7D

[redacted]

Investigation on 07/18/2002 at Chicago, Illinois

File # [redacted] Date dictated 07/19/2002 b6 b7C b7D

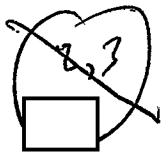
by SA [redacted] b7E

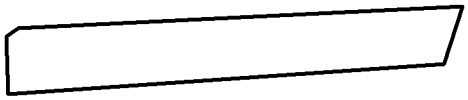
This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 1
Page 2 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX





b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1422587-000

Total Deleted Page(s) = 2
Page 4 ~ b6; b7C; b7D; b7E;
Page 5 ~ b6; b7C; b7D; b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

The USSS investigation has revealed that numerous Government and private sector computer systems have been subject to attack over the past years. Rather than the "hackers" keeping stolen computer files on their own personal computers, the "hacker" group uses the computer systems they invade to store programs and files they steal. Several systems have been used in this manner before. It has been determined that the LEGION OF DOOM organization also uses a Turkish government computer system called ARMA in Ankara, Turkey, to store computer files, specifically, a copy of the November 1989 Phrack Journal.

The LEGION OF DOOM involves a tightly knit core group of about 15 individuals who are from 21 to 22 years of age and whose primary reason for affiliation is to gather information for and then publish a "hackers" magazine called "PHRACK 2600". The LEGION OF DOOM is loosely affiliated with other "hackers" from both the United States and overseas, contacts noted as being primarily in England, Germany and Australia.

The Knoxville Office has a listing of the members of the LEGION OF DOOM which lists 60 known members of this organization. Also listed in this organization were [redacted] aka [redacted] and [redacted] aka [redacted] has five telephone lines, [redacted] located in Lockport, Illinois, which is used in the transfer and storage of the E911 file involved in the February 1990, USSS case. It should also be noted that this same individual, [redacted] aka [redacted] is the same individual identified as one of the "hackers" in the Knoxville COLONIAL FREIGHT case, still using the same handle of [redacted]

b6
b7C

Memorandum

To : SAC, KNOXVILLE (264A-KX-61179) (P) Date 6/30/92

From : SA [redacted] b6 b7C

Subject: UNSUB(S);
COLONIAL FREIGHT SYSTEMS,
KNOXVILLE, TENNESSEE -
VICTIM;
JANUARY 1990 - DECEMBER 1991;
COMPUTER FRAUD AND ABUSE -
IMPAIRMENT;
OO: KNOXVILLE

The purpose of this memo is to give background information on captioned case and to give an update into this ongoing investigation. On 1/13/92, captioned investigation was opened after the Knoxville Office received a telephone call from COLONIAL FREIGHT TRUCKING COMPANY (victim company) that someone had entered their computer system and had access to their telephone lines without authorization. The Knoxville FBI Office checked into the matter and immediately realized that Unknown Subject(s) (UNSUB(s)) intentionally modified the COLONIAL FREIGHT SYSTEMS network by gaining "super-user" access to the operating system, placing copyright software on the computer, unlawfully using the telephone circuits, and otherwise effecting the normal operations of the computer.

COLONIAL's computers are located in five states: Texas, North Carolina, New Jersey, Georgia, Ohio, and Tennessee. Therefore, COLONIAL's network qualifies as a "Federal Interstate Computer", under Title 18, United States Code, Section 1030(e)(2)(B) since it is one of two or more computers used in committing the offense, not all of which are located in the same state.

The intruder(s) exceeded authorized access since he/she accessed COLONIAL's computer without authorization to obtain an alter information that the accessor is not entitled to obtain or alter (Title 18, United States Code, Section 1030(e)(6).

[redacted]
(2)

264A-KX-61179-43

SEARCHED [redacted] DEXED
SERIALIZED [redacted] ED
JUN 30 1992
FBI — KNOXVILLE

b6 b7C